CIP Four-Year Strategic Plan

Fiscal Years 2024 - 2027

Office of the Chief Security Officer
Cybersecurity and Infrastructure Protection
Michigan Department of Technology, Management & Budget

Mission Statement

Enable the business to function securely while making security easier for customers and harder for hackers.

Vision Statement

Cybersecurity and Infrastructure Protection (CIP), operating as Business Services, Identity and Architecture (IA), Michigan Security Operations Center (MiSOC), Office of Infrastructure Protection (OIP), and Risk Compliance and Delivery (RCD), will bring a compassionate and empathetic approach to provide digital and infrastructure security services to our customers within state employment, state agencies, and the public by delivering world-class services and providing great customer service.

Goals

CIP division-wide goals will map to the DTMB strategic goals and DTMB IT strategic goals to ensure alignment with the overall strategic mission of DTMB.

Objectives

- Reconcile tools used across the divisions to track compliance with DTMB policy, standards, and procedures to ensure planning for lifecycle events, such as authority to operate (ATO), contract renewals, and potential migrations to new products, are planned and managed in advance of end of life and end of contract situations.
- Ensure onboarding and offboarding procedures are created that assist employees and contractors be successful beyond day one with topical onboarding and training plans by work role and duties.
- Ensure a DTMB and CIP best practices guide is created that informs employees and contractors of how Michigan government functions and details their role as a member of CIP.

Business Services

- Provide financial planning, purchasing, analysis, and reporting of the budget to CIP division directors. Further development of separation of financial reporting by division directors.
- Provide continued human resources support and onboarding and offboarding guidance and assistance to all of CIP. Continue to streamline and implement workflows that will further improve all HR related processes.
- Consistently provide useful and clear communications to internal and external audiences on a variety of topics relating to CIP.
- Continue to support CIP reporting through the growth of the CIP Data Analytics Program (CDAP) and support other CIP Divisions with controlled data sharing and automation services using low-code/no-code systems development.
- Develop a CIP Student Services program to support workforce development within DTMB.
- Introduce a CIP Business Analytics Services to support division area project management.

External Engagement

- In conjunction with Business Services, manage the Michigan Cybersecurity External Engagements services, including Michigan's State and Local Cybersecurity Grant Program (SLCGP), CSO Kitchen Cabinet, Michigan Cyber Civilian Corps (MiC3), Michigan Cyber Partners, Cybersecurity Resource Hub, Michigan Secure App, Cyber Traveler, Michigan Cyber Summit, Governor's High School Cyber Challenge, Elections Security with ES-ISAC engagement and support events, as well as other symposiums, summits, speaking engagements, and outreach across CIP.

Identity and Architecture

- Continue to support implementation of the MiLogin Roadmap and begin to include new opportunities to provide identity services to local governments and non-state government customers supported by our external engagement practices.
- Provide support for security liaisons, MiSOC, procurement, enterprise architecture, and cloud adoption in compliance with existing and new policies, standards, and procedures.
- Continue to grow the Secure Application Development Lifecycle (SADLC) team and services in support of Zero Trust Architecture and Development Security Operations (DevSecOps) best practices.

Michigan Security Operations Center

- Embrace automation and cloud platforms supplemented by artificial intelligence (AI) to keep pace with and scale our identification, detection, prevention, response, and recovery capabilities as the generative transformer platform future of AI begins to affect our services.
- Seek opportunities to expand usage of existing and new tools in support of Zero Trust Architecture principles that enforce just-in-time access control provisioning and deprecate reliance on static implicit trust-based access controls, in which these systems include secure service edge platforms and extended managed detection and response tools.
- Establish ongoing engagements with external partners including, but not limed to, DHS, CISA, Michigan National Guard cyber divisions, FBI, MS-ISAC, North Dakota JC-SOC, New Jersey Cybersecurity & Communications Integration Cell, and Louisianna Universal SOC with a long-term objective of establishing a Michigan Universal SOC.

Office of Infrastructure Protection

- Manage the emergency services, building access, and building security services necessary for state infrastructure to provide safe and secure working environments.
- Own security awareness and training, tabletop exercises, and DTMB continuity planning, including CIP workforce specific training based on the NICE framework[1] where appropriate and training supplemented by other sources, such as the National Cyber Workforce and Education Strategy[2], that enable role-based career paths and growth.

Risk Compliance and Delivery

- Continue efforts to streamline and improve the Michigan Security Accreditation Process (MiSAP) automation workflows to increase understanding of and reduce risk across all State of Michigan applications.
- Take ownership of the 1340.00 Information Technology Information Security Policy and supporting standards to reconcile MiSAP automation to updated policy and standards and complete the process of rationalizing the updated policies through the review and comment process associated with the cross functional review team (CFRT) within the Office of Performance Management related to Administrative Guide to State Government policy management.
- Provide support to agencies in gathering relevant control evidence during the MiSAP process and the Internal Control Evaluation (ICE) audits. Guide agencies in achieving successful results in various audits and federal compliance assessments of their programs.
- Establish consistent communication with agency security officers, business relationship managers, and agency IT liaisons to provide them information from other CIP divisions about the status and operational risks carried within the business applications they utilize to serve their customers to include vulnerabilities, incident response liaison with MiSOC, and MiSAP plan of action and milestones (POAM) management.

[1] https://niccs.cisa.gov/workforce-development/nice-framework

[2] https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/31/fact-sheet-biden-%e2%81%a0harris-administration-announces-national-cyber-workforce-and-education-strategy-unleashing-americas-cyber-talent/